5-12-1998

How are hospitals disseminating their patient confidentiality policies to their employees?

Sally Sapega
Rowan University

How are Hospitals Disseminating Their Patient Confidentiality Policies to Their Employees?

by
Sally Sapega

A Thesis

Submitted in partial fulfillment of the requirements of the
Master of Arts Degree in the Graduate Division
of Rowan University
May 15, 1998

Approved by _____

Date Approved 5/12/98

ABSTRACT

Sally Sapega

How are Hospitals Disseminating Their Patient Confidentiality Policies to Their Employees?

1998

Larry Litwin

Corporate Public Relations

Depending on a patient's illness, as many as 100 health professionals and administrative personnel may have access to the hospital record, all with a legitimate reason. Many people are understandably concerned about confidentiality because of the range of information in medical records that is often necessary to ensure an accurate diagnosis and successful treatment -- including very personal information about a person's physical, mental, and sometimes even emotional well-being. This thesis examined how 20 Delaware Valley hospitals communicate their patient confidentiality policies to their employees. The survey specifically asked the channels through which their confidentiality policies are communicated (ie, training programs or memos) as well as what messages are communicated. The results were recorded through percentages. Based on results, it appears that patient confidentiality is taken seriously in most hospitals and specific measures have been implemented to ensure that hospital employees understand just how easily confidentiality can be breached and how it can be protected.

MINI-ABSTRACT

Sally Sapega

How are Hospitals Disseminating Their Patient Confidentiality Policies to Their Employees?

1998

Larry Litwin

Corporate Public Relations

Today's medical records contain a wide range of information, including a patient's physical, mental, and sometimes even emotional well-being. This type of information, combined with the number of people who have access to a patient's medical record, makes patient confidentiality essential. Hospitals are responding to this by training their employees how to keep this information private and avoid potential breaches.

ACKNOWLEDGEMENTS

I dedicate this thesis to my family and friends for their love and support, and to my advisor, whose humor and unending encouragement brought me to a successful finish.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

"Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets."

- Oath of Hippocrates, 4th Century, B.C.E

When Hippocrates wrote this oath, patient confidentiality was a simple process. The patient told his/her symptoms to the doctor, and the doctor took care of them. There were no employees, insurance companies, or computers to deal with.

Today, this is no longer the case. Now, depending on a patient's illness, at least 25, and possibly as many as 100, health professionals and administrative personnel may

have access to the hospital record -- all with a legitimate reason to see that record.[1]

Many people are understandably concerned about the potential for breaches of confidentiality. In fact, the Harris-Equifax Health Information Privacy Survey of 1993 showed that 80 percent of the American public is worried about their personal privacy.[2] And in the case of medical records, it's easy to understand why.

The range of information in medical records -- very personal information about a person's physical, mental, and sometimes, even emotional well-being -- is overwhelming. In addition to diagnostic and testing information, the medical record may include the details of a person's family history, genetic testing, history of diseases and treatments, history of drug use, religious observances and their impact on treatment decisions, dietary habits, exercise and recreational activities (including dangerous ones life insurers would want to know about), and sexual orientation and practices. Subjective remarks about a patient's demeanor, character, and comments on attitudes toward illness, physicians, treatments, compliance with therapy and advice may also be part of the record.[3] Such medical information can affect such basic life activities as marriage, career, obtaining insurance, or driving a car.

This range of information is often necessary to ensure an accurate diagnosis and

---

1 Siegler, M. (1982). Confidentiality in medicine: a decrepit concept. New England Journal of Medicine, 307, 1518-21.

2 Simpson, R.L. (1994). Ensuring patient data privacy, confidentiality and security. Nursing Management, July, 18-20.

3 Carpenter, J. (1997). Answers to confidentiality concerns. In Confidence, 5(5), 43.

successful treatment. But would patients be willing to share this information if they feared it wouldn't be kept confidential?

Computerization, which simplifies access to records, is compounding the problem. To counter the easy accessibility, security measures have become more technically advanced. In addition, there are now laws governing the dissemination of sensitive material, including information on genetic testing, HIV, and substance abuse.

But, although technology can secure information, it cannot stop people from talking or from making careless mistakes.[4] And the situations that lend themselves to these breaches are numerous and diverse.

For instance, in one case, a doctor requested the records from a psychologist of a mutual patient. The information was faxed to the patient's place of employment instead.[5] In another situation, there were two patients with the same last name on the same ward; one had renal failure, the other a kidney disorder. The first needed a transplant but the family requested that they be allowed to break the news. The nurse jotted down a note, left it out in the open and then was paged. The second patient saw the note and became hysterical. Although she was quickly told of the mistake, it could easily have been avoided.[6]

4
Hard, R. (1992). Keeping patient data secure within hospitals. Hospitals, 66(20), 50.

5
Sharp, H. (1994). Letter to Editor. Journal of the American Medical Association, 271(18) 1401-02.

6
Smith, J. (1995). Patient confidentiality: prying eyes. Nursing, 25 (9), 26.

Confidentiality can also lapse internally, from one hospital employee to another. For example, a nurse from one unit went to another unit to inquire about her neighbor's condition in the oncology unit. Even though the neighboring nurse had good intentions, the oncology unit nurse did not give out the information. Safeguarding confidentiality is more important than professional courtesy.[7]

Other circumstances leading to unauthorized disclosure include conversing about a patient in an open area, releasing information through phone conversations to unauthorized parties, or even leaving an overly descriptive message on an answering machine.

Not surprisingly, these confidentiality slips are not rare. In reality, incidents involving patient embarrassment from disclosed information occur in this country once or twice a week.[8]

Disclosures of this sensitive information can go further than embarrassment, however. They can lead to loss of one's job, loss of one's insurance coverage, and damage to a career or profession.[9] For example, Senator Thomas Eagleton ended his campaign for vice president in 1972 after it became known that he had been treated for

---

7 Salladay, S.A. (1994). Patient confidentiality: on the spot. Nursing, 24 (8), 29-30.

8 Lawrence, L.M. (1994). Safeguarding the confidentiality of automated medical information. Joint Commission Journal on Quality Improvement, 20 (11), 639-646.

9 same as above.

mental illness.[10] And Arthur Ashe's tragedy highlights even more the adverse effect of broken confidentiality.

Disclosures may also go beyond personal repercussions; they may lead to lawsuits. One patient sued a hospital, claiming that on two occasions different hospital employees discussed her medical condition, without her consent, with her husband and ex-husband.[11] Another involved a surgeon who was diagnosed with AIDS. His chart was kept at the nurse's station at a hospital with no special protection and his condition soon became widely known. The doctor sued the hospital for its failure to take reasonable steps to protect his confidentiality.[12] The standard for judging a breach of confidence is clear: You can be found liable for any unauthorized disclosure of patient information that "offends the sensibilities of an ordinary person."[13]

Of course, there are times when releasing sensitive information is for the patient's welfare. Hospital employees are required to report incidents of rape, and other criminally inflicted injury, abuse or neglect to the appropriate authorities. Hospital employees need to be trained and to differentiate what must legally be reported versus what must remain

---

10 Lawrence, L.M. (1994). Safeguarding the confidentiality of automated medical information. Joint Commission Journal on Quality Improvement, 20 (11), 639-646.

11 Legal action involving breaches of patient confidentiality, Irongate, Inc., http://www.irongateinc.com//lawsuits.html.

12 same as above

13 Greve, P. (1990). Keep quiet or speak up? Issues in patient confidentiality. RN, 53 (12), 53.

confidential.

It's important to note that not every breach is unintentional. A case study told of a disgruntled nurse who learned a doctor's password and proceeded to prescribe heart medication for a juvenile (which was luckily intercepted) and antibiotics to a geriatric patient, and to order discharges of a patient who wasn't ready. In addition to all the potential harm to patients, the doctor paid a steep price; he was sent to jail. Obviously, no amount of training can prevent this type of retribution.[14]

The Hippocratic Oath stresses to physicians the importance of confidentiality. And, nurses, too, have a history of protecting patient confidentiality. In 1950 the American Nurses Association adopted a code that said "The nurse safeguards the client's right to privacy by judiciously protecting information in a confidential manner."[15]

While physicians and nurses are comfortable with this responsibility, others in the health care information system (unit clerks, receptionists, billing staff, etc) may not have been formally exposed to a code of ethics regarding patient information.[16] According to one source,"All people involved with patient-specific healthcare information must be bound by an ethical code and must have regular training in ethics and privacy issues."

---

14 Simpson, R.L. (1994). Ensuring patient data, privacy, confidentiality, and security. Nursing Management, July, 18-20.

15 Milholland, D.K. (1994). Privacy and confidentiality of patient information. Journal of Nursing Administration, 2, 19-24.

16 Coleman, M.T. (1995). Ensuring patient confidentiality. Journal of Family Practice, 40 (1), 18.

There must be policies and procedures relevant to protecting access to records - policies or procedures for blocking sensitive data.[17]

So what are hospitals doing to try and stem this unauthorized flow of information?

This study will investigate a number of area hospitals' policies that address patient confidentiality. By use of a survey, this study will determine the following trends:

* Do hospitals have specific training programs to communicate the importance of confidentiality to all their employees?

* Do they rely simply on a written statement that is read and signed?

* Is confidentiality training an ongoing program or does it stop after orientation?

* Is training required for all levels of employees and, if so, is it the same program?

At the University of Pennsylvania Health System, a task force has been studying this topic. For several months it has been meeting regularly to establish an ongoing 'confidentiality' program, which will include handouts for employees, videos on how breaches occur and how to handle these situations, and HUSH signs throughout the medical center, reminding all employees of their role in guarding this information.

The key to confidentiality, then, is a well-trained staff, good policies and procedures, and safeguards.

Delimitations

This thesis will not deal with security measures to safeguard computerized records

---

17 Milholland, D.K. (1994). Privacy and confidentiality of patient information. Journal of Nursing Administration, 2, 19-24.

(ie, passwords) or with intentional breaches of confidentiality. Nor will it discuss ethical decisions of confidentiality that doctors must make when the safety of the patient or friends and family are at stake. The majority of hospital employees will never face this type of test.

This thesis will only describe hospitals' approaches to protecting patient confidentiality by properly training employees.

Definition of Terms

Confidentiality - Restriction of access to data and information to individuals who have a need, a reason, and permission for access.

Patient Confidentiality - Restriction of access to specific health care data relating to each patient to those who have a medical need, reason and permission.

Health System - A group of hospitals

Medical Record - Information or an account of facts, set down in writing, as a means of preserving knowledge of all information pertaining to a person's health.

Access - The ability to get health care services or information.

Joint Commission on the Accreditation of Health Care Organizations - A national organization that accredits health care organizations and agencies.

CHAPTER II

LITERATURE REVIEW

Data Sources

The source of data in this study included the health science data bases of the University of Pennsylvania School of Medicine: MEDLINE, Bioethics Line, CINAHL/Nursing, Full-text Core Biomedical Journals, as well as the Franklin Library catalog. Data was also retrieved from SearchBank and the Internet.

The key words used with the most successful results were patient confidentiality, hospital employees/staff and training.

Confidentiality: A Growing Priority

As advances in technology continue and medicine itself undergoes drastic changes, patient confidentiality is becoming increasingly important, in the minds of both the health care industry and the consumer/patient.

The team approach in patient care, which now includes both medical and nonmedical personnel, is certainly a stumbling block to confidentiality. And while technology has improved patient care through easy access to records and medical

information, it has also made breaching these confidences that much easier as well.

The confidentiality of computerized medical records was a topic of several articles. One article proclaimed that "the biggest challenge today is unauthorized access."[1] Even 'authorized' access is causing concern. After all, it's one thing for a doctor to have instant access to medical records; it's another thing for a potential employer to see them.

Where are the Breaches Occurring?

Although computerized medical records present a challenge in protecting patient confidentiality, literature shows that it is more often other sources of communication that give way to security gaps. For example, the ease of mis-faxing was mentioned in several articles. One described the case involving a pregnant hospital employee with herpes whose medical records were mistakenly faxed to her co-workers instead of to the doctor.[2]

Other sources of breaches described in the literature included open charts available for anyone to see, original records left on the copier, and sensitive messages left on an answering machine. Unauthorized release of information also is a significant source of confidentiality breaches. But, by far, conversations by healthcare professionals, overheard by other people, are the biggest source.

As one article states,"Verbal breaches of confidentiality are the classic cases of

---

1 Simpson, R.L. (1994). Ensuring patient data, privacy, confidentiality and security. Nursing Management (July) 18-20.

2 Sharp, M.S. (1994). Letter to the Editor. Journal of the American Medical Association, 271 (18) 1401-1402.

wrongdoing. Although health care professionals learn early in their education about the dangers of spoken breaches, these admonitions are not always heeded."[3] It's not so surprising then that an early study (1982) among physicians, medical students and patients found that, while only a minority of patients believe their cases should be shared with other non-involved people, more than half of the doctors indicated that such discussions occur frequently.[4]

Healthcare security has also been in the news. Articles from newspapers throughout the country have shown how poorly protected much of our health care information is. For example, one *Boston Globe* article ("Patients' Files Allegedly Used for Obscene Calls") told of a hospital employee who used a former employee's password to gain access to nearly 1,000 confidential patient files. A 1996 *Time* magazine article ("Who's Looking at Your Files?") also expressed consumers' concerns that sensitive, personal information in medical records might be available to employers or insurers.

One of the more famous confidentiality studies that made news was the 'elevator study' in which it was shown that doctors consistently discussed confidential patient information on elevators, regardless of other people being present.[5]

3

Dowd, S and Dowd, L. (1996). Maintaining confidentiality: Health care's ongoing dilemma. Health Care Supervisor 15 (1) 24-31

4

Weiss, B. (1982). Confidentiality expectations of patients, physicians, and medical students. Journal of the American Medical Association, 247. 2695-97.

5

"News Articles Related to Healthcare Information Security," Irongate, Inc. http://www.irongateinc.com/articles.html.

What Are the Laws?

While some federal laws address the question of privacy in certain information collected and maintained by the federal government, no federal statute defines an individual's specific right to privacy in his or her personal health care information held in the private sector and by state or local governments.[6]

Laws protecting the confidentiality of health care information vary markedly from state to state. In some states there are little or no statutory requirements for health care providers and institutions to protect the confidentiality of health care information. [7]

In Pennsylvania, currently, no one law addresses the overall area of patient confidentiality. Rather, separate laws exist to protect specific areas:

* HIV-related information (HIV-Related Information Act states that..."physicians, their employees and agents are required to maintain the confidentiality of all HIV-related information...whether the information is disclosed voluntarily, involuntarily, or pursuant to Court order.")[8]

* drug and alcohol records (Pennsylvania Drug and Alcohol Abuse Control Act states

---

6 The right to privacy in health care information. Office of Technology Assessment, http://www. eff.org/pub/privacy/medical/1993_ota_medical_privacy report.

7 Gostin, L.et al.(1997) "Legislative Survey of State Confidentiality Laws with Specific Emphasis on HIV and Immunization," http://www.epic.org/privacy/medical/cdc_survey.html

8 McKissock & Hoffman, PC. (1992). Laws and regulations affecting medical practice: A guide for Pennsylvania physicians, June, 24.

that "all patient records...relating to drug or alcohol abuse, or drug or alcohol dependency, prepared or obtained by a private practitioner, hospital, clinic, drug rehabilitation, or drug treatment center are confidential")[9]

* mental health records (Mental Health Procedures Act prohibits "the disclosure of privileged information without the patient's consent...")[10]

* physician-patient privilege. (As set forth in Pennsylvania's statues, it reads that "No physician shall be allowed, in any civil manner, to disclose any information which he acquired in attending the patient in a professional capacity... without consent of the patient...") [11]

In New Jersey, there is a bill of rights for hospital patients, which provides the right "to privacy and confidentiality of all records pertaining to his treatment..."[12] There are also statutes protecting confidentiality of treatment of alcohol abuse[13], AIDS [14], and

---

9 McKissock & Hoffman, PC. (1992). Laws and regulations affecting medical practice: A guide for Pennsylvania physicians, June, 63.

10 McKissock & Hoffman, PC. (1992). Laws and regulations affecting medical practice: A guide for Pennsylvania physicians, June, 64.

11 McKissock & Hoffman, PC. (1992). Laws and regulations affecting medical practice: A guide for Pennsylvania physicians, June, 59.

[12]NJ Statute 26.2H-12.8.

[13]Records; confidentiality; rights of patients, NJ Statute 26:2B-20.

[14]Record of identifying information; confidentiality, NJ Statute 26:2B-20.

mental health [15], and the physician/patient privilege[16]. For drug abuse, the author could only find a statute of "confidentiality regarding therapeutic research of controlled dangerous substances."[17]

Hospital Stipulations Protecting Confidentiality

In addition to keeping within state and federal laws, hospitals are also bound by the stipulations of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), an organization which measures how well U.S. hospitals are managed in several areas, one of which is confidentiality. According to the Comprehensive Accreditation Manual for Hospitals, a hospital must "maintain the security and confidentiality of data and information, and is especially careful about preserving the confidentiality of sensitive data and information... Policies and procedures, based on applicable law and regulation, address confidentiality of patient information. The patient is informed of the hospital's policy on confidentiality at the time of admission."[18]

There are also specific codes of ethics for certain health care professionals -- physicians and nurses -- that stress confidentiality.

---

[15] Confidential nature of certificates, applications, records and reports, NJ Statute 30:4-24.3.

[16] Patient and physician privilege, NJ Statute 2A.84A-22.2.

[17] NJ Statute 26.2L-4.

[18] Management of Information (1996). Comprehensive Accreditation Manual for Hospitals, pg. IM-10.

Confidentiality Training

Most of the available literature stresses the importance of patient confidentiality and is filled with examples of how it can be breached. Some articles contain recommendations or solutions to specific problems (ie, "Maintaining patient confidentiality in the emergency department"[19] and "FAX guidelines protect patient confidentiality"[20]). The author also found one publication, *INConfidence* (a monthly newsletter of the American Health Information Management Association), that seems to deal exclusively with all areas of patient confidentiality.

However, little was found on how to communicate the importance of this information -- and the consequences of breaches -- to hospital employees, ie, an overall program touching on all of the problematic areas. The alert is out but the overall solutions or recommendations are lagging behind.

---

19 Howell, M. (1996). Maintaining patient confidentiality in A & E. Nursing Times, 90, (34) 44-45.

20 Koska, M.T. (1992) Outcomes research: hospitals face confidentiality concerns. Hospitals, 66, 32-33.

CHAPTER III

METHODS AND MATERIALS

Data Needed

This investigation revealed if hospitals have patient confidentiality policies and how they communicate these policies to employees. The research determined specific methods used to communicate this information to employees, the frequency of this communication process, and the differences, if any, of this training among the different levels of employees.

Means of Acquiring Data

A pretest was done with an employee at the University of Pennsylvania Health System who works in Market Research. To assure a high percentage of responses, the survey was as short and simple as possible, while including all necessary data.

The survey revealed:

* which employees receive training

* how often this training is done

* what areas of confidentiality are covered in training

The final study was limited to 20 hospitals in New Jersey and Pennsylvania. However, an initial list of over 30 hospitals was compiled in the event that some hospital employees felt uncomfortable about supplying the necessary information (although they were ensured that their information would be kept strictly confidential). Urban and suburban hospitals, academic and non-academic, were chosen from the Yellow Pages.

Based on the answers and input received after questioning the first few hospitals, the original survey was modified. Some questions were changed or clarified; others were added to increase the range of information. The initial hospitals were later recontacted to get this additional information to include in the survey.

The appropriate contact in each hospital was found either through an established contact in that hospital or, if none was available, by asking hospital operators for the department dealing with patient relations. The department responsible for communicating the patient confidentiality policy to employees varied greatly among the various hospitals, from human resources to patient relations to quality management.

All but two of the interviews were taken over the phone. Both of these respondents requested that the survey be faxed to them, so they could complete it when they had some spare time. The total time for completing the survey during the telephone interviews ranged from 10-20 minutes.

Participating hospitals were offered a finished copy of the survey results or the entire thesis.

CHAPTER IV

ANALYSIS OF DATA

Twenty hospitals in the Delaware Valley were surveyed on how they communicate their patient confidentiality policies to their employees. The survey specifically asked the channels through which their confidentiality policies were communicated (ie, training programs or memos) as well as what messages were communicated.

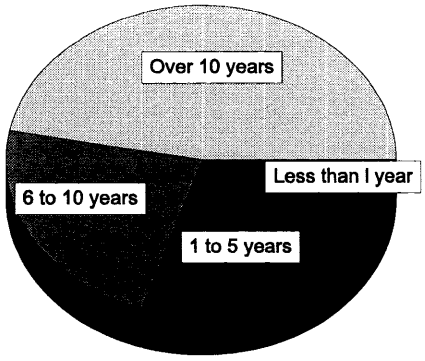
The hospitals chosen were located in both urban and suburban areas. There was a wide range in the number of employees per hospital and the size of the hospital itself: employees numbered from 700 to 4000, and hospital size ranged from 100 beds to over 1000.

Ninety percent of the surveys were administered via the telephone. The remaining two hospitals requested a faxed version which they filled out and returned.

All of the hospitals offer confidentiality awareness in one form or another, some in more depth than others.

In answer to question one, 84 percent of hospitals surveyed have a formal policy while the remaining hospitals include confidentiality as part of clauses in the general hospital policy. In half of those surveyed, the formal policies or confidentiality clauses have been in effect for over 10 years. Twenty-five percent have had policies/clauses for the past 6-10 years and the remaining group for less than five years.

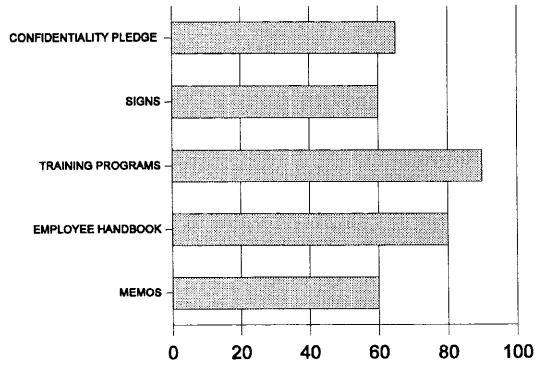
AGES OF CONFIDENTIALITY POLICIES



How is the Information Communicated?

According to the responses, many channels are used to communicate a hospital's confidentiality policy to employees. The survey listed five potential sources: memos, employee handbook, training program, signs throughout the hospital and confidentiality pledges requiring signature. The majority of hospitals offer more than one means. Whether the hospital has a formal policy or general clauses, the majority of communication is done through employee handbooks and training programs. Sixty percent also use memos, in-hospital signs, and

CHANNELS OF COMMUNICATION



confidentiality pledges. (Examples of confidentiality signs are on pages 24-25.) Only two hospitals include all five methods, while nearly half use four of them.

In addition to the channels mentioned, the survey also asked for any other methods of communicating this information. One hospital also includes a confidentiality liaison in each department who surveys department members and reviews confidentiality issues.

Memos

Of those hospitals that use memos to communicate this information, one-third include physicians in their distribution list while one-quarter of those surveyed send copies solely to department heads to post or distribute. The remainder distribute to all employees.

Slightly less than half of those who distribute memos to all employees required a signature to confirm that the memo was received and read. Most of that group included physicians in their distribution.

Employee Handbooks

Of the 80 percent of hospitals that put confidentiality information in employee handbooks, the majority (75%) distribute these handbooks to everyone, including physicians. Twelve percent send to all employees but physicians, and the remaining hospitals send handbooks to non-nursing personnel or supervisors only. Less than half are required to sign off on receiving and reading the information.

Training Program

Training programs are popular; ninety percent of hospitals surveyed use them as one way to disseminate confidentiality information. However, the frequency of training programs is almost evenly divided between orientation only, and at orientation and on an annual basis. Neither the size of the hospital nor the location (ie, suburban vs urban) seemed to affect the frequency.

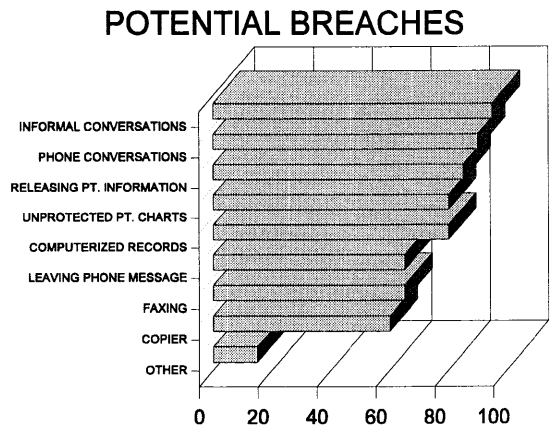
One-third have used this training program over five but less than 10 years while another third have over a year but less than five years' experience. Two of the hospitals had only recently (less than a year) begun using their programs. Nearly all of them use oral presentation and 67 percent add videos to this presentation. Other methods of communicating this information in a training program include role playing, self-tests, and passing out pamphlets or other handouts. Nearly 90% developed the programs in-house; the remaining hospitals went through a consulting firm.

Who receives this method of training? Fifty-six percent make it mandatory for all employees, including physicians. The rest do not require physicians to attend, even as part of orientation.

Most hospitals offer the same confidentiality training for all employees who receive the training; only a minority of the hospitals alter it according to department or position. For example, one hospital makes it department-specific, another uses clinical and nonclinical versions, while a third has a basic training program but gives medical records a more thorough training.

Potential Breaches

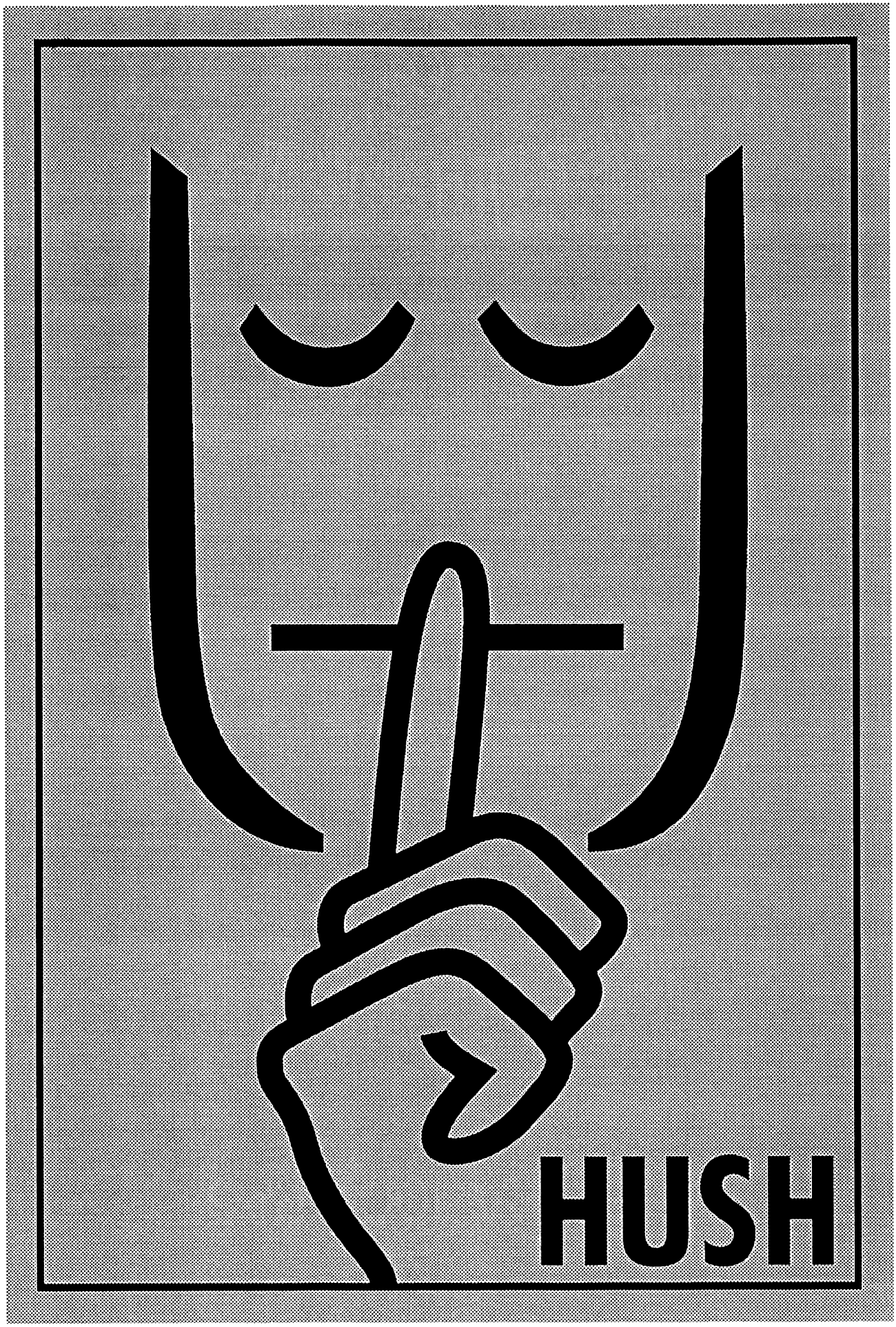
Question 14 asked specifically which areas of potential breaches are covered in the confidentiality training, regardless of the channels used in disseminating the message. Ninety-five percent discuss breaches occurring during informal conversations in the hospital (ie, hallways, cafeteria, elevator) and 90 percent cover phone conversations by employees that could be overheard by patients or their families. The unauthorized release of patient information is discussed in 85 percent of hospitals but most just tell employees to refer all requests to medical records. Protecting patient charts and computerized records were included in 80 percent of training. At least 60 percent of the hospitals also review confidentiality issues involving leaving messages on a patient's answering machine, faxing, and use of copiers (ie, leaving confidential material in the copier). In addition to the above mentioned topics, one hospital discusses e-mail misuse, and another warns about the dangers of talking in shuttle vans, records being sent to the wrong person, or bringing patient information home and sharing it with the employee's family. The majority of hospitals covered multiple topics in their training channels but, of the 20 surveyed, one hospital *only* covered the confidentiality risk with computerized records.



Some of the hospitals (60 percent) addressed how to handle an authorized release

of information, ie, to legal recipients such as other hospitals and care providers, insurers, or in response to subpoena. Thirty percent felt this was more department specific training and left that training for employees who would most likely be responsible for this request, including employees in nursing and medical records.

Eighty percent of hospitals specify the consequences of breaching confidentiality in their policy (which range from a discussion with the employee to dismissal) and 94 percent of these hospitals communicate this plan to their employees.


HUSH

BE
AWARE

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Summary

Twenty hospitals in the Delaware Valley were surveyed to determine how they communicate their confidentiality policies to their employees. All but two of the surveys were done through telephone interviews.

Many of the survey's questions focused on the actual channels of communicating confidentiality messages -- training programs, signs, memos, confidentiality statements, and employee handbooks -- and to which audiences these messages are sent.

A smaller segment zeroed in on what messages are communicated. There are many ways to breach confidentiality (for example, through faxes, phone messages, and computers). Usually, these slips are unintentional. An employee may not realize that he or she is actually violating a patient's confidentiality. Respondents were asked how many of these methods are covered in the hospital's training.

Conclusions

As more and more people have access to personal medical records, protecting confidentiality has become more important. The sensitive nature of this information makes it essential for hospitals to train employees properly to protect it.

The results of the survey show that most hospitals in this region are taking confidentiality training very seriously. The majority schedule confidentiality training programs during orientation and more than half do this training on an annual basis. All but one disseminate this information through at least three channels. The most popular is the training program. Many of the hospitals that use this method combine oral presentation, videos and handouts, reinforcing the message through multiple means. One hospital puts timely reminders in the hospital newsletter, which goes to every employee.

The one significant finding is that physicians are often excluded from this confidentiality training. In some hospitals, this reflects employee status, ie, physicians may not be considered 'employees' but rather independent consultants. Or, hospitals may assume that the Hippocratic Oath, which stresses confidentiality, is a part of every physician's training and so they do not need the additional instruction. However, the literature shows that it is often the physician who unwittingly breaches confidentiality, by speaking openly -- in a very public place-- to a another doctor or to a patient directly. As examples in this thesis prove, these seemingly innocuous events can lead to disastrous results.

While it is obviously important to stress confidentiality to employees who work directly with patients, it is equally essential for those who do 'behind the scenes' work and

many hospitals seem aware of this. In most of the surveyed hospitals, training is given to all employees, including administrative and maintenance workers. Some hospitals offer the same training to everyone. Others use department specific training, depending on the level of contact with patients and their medical information. For example, one hospital uses two different versions of a training video, for clinical and nonclinical employees. In another hospital, maintenance workers receive "a sentence or two" on confidentiality while those with direct access to patient information or patient care, such as medical records, admissions, nursing, and labs, are given the most training. This particular hospital relies on department supervisors to review confidentiality annually as part of an employee's evaluation.

In almost every hospital surveyed, the medical records department's employees receive the most confidentiality training. Survey results show that it is common to train employees to refer all legal requests for patient information to this group.

When memos are part of the dissemination process, one-quarter of the respondents only send it out to department managers who then post it. In all hospitals, this, along with confidentiality pledges and signs, are used only as an adjunctive method, to reinforce stronger channels.

Results show that hospitals are taking steps to help overcome some of these breaching problems. To protect patient confidentiality in the emergency room, one hospital has added new cubicles that are designed to provide more privacy. Another has doctors give surgical results in a nearby chapel, no matter what the results.

Recommendations

Based on the conclusions of the study, there are several recommendations to ensure the confidentiality of patient information. Foremost, it's essential that all medical and nonmedical personnel be included in the training. It's obvious that people working with patient information need to learn confidentiality rules. However, even those people who have no direct patient contact but who have reason to be in the patient area (such as maintenance) should be taught the dangers of passing on information. In one training video that the author viewed, a scenario showed a doctor speaking with a patient in her room, while a maintenance person was present. Since he recognized the patient, the maintenance person then passed on the information to his family. Although the doctor was wrong to speak when the patient was not guaranteed privacy, it was equally wrong for the other employee to spread the information around. An employee who has no 'hands on' exposure to patients may not be aware that repeating an overheard conversation between a doctor and patient is as much a breach as directly reading the records.

Confidentiality training should include doctors and nurses (although they are also taught confidentiality practices in school). The elevator study[1] demonstrated that confidentiality is often the last thing on a medical person's mind when discussing a patient with a peer. Although input from other staff members may be a necessary part of treating a patient, it should be done in the privacy of an office.

---

1 Ubel, P., Zell, M., et al. (1995). Elevator talk: Observational study of inappropriate comments in public spaces. American Journal of Medicine, 99 (2), 190-94.

Even off-site locations may not be safe to discuss patient matters. Another video scenario showed two doctors discussing a patient (who happened to be an employee) in a restaurant local to the hospital. They were overheard by another employee and the news traveled fast among her coworkers.

No matter what method of training is used, it's crucial that employees understand the importance of protecting confidentiality of co-workers who are hospitalized. A person's health is a private matter and no matter how well-intentioned an employee is, he or she should not ask for or receive medical information about a coworker.

Actual training programs -- with oral presentations and videos -- should be done at every hospital. It is an excellent way to ensure that all employees are exposed to this information. Sending out memos or putting up signs alone is by no means an effective method of communicating, especially if an audience is not that interested in the topic to begin with. These methods should only supplement information given during active training.

One way to get employees more involved (and thus more likely to retain the information) is to give them some input into how these programs are run and allow them to actively participate in the training, not just sit as a passive audience. A few of the hospitals tried role playing to aid in retention.

This training should be done on an annual basis. Although it is smart to include confidentiality training during orientation, it is just one of many topics that are covered on those days. The consequences of broken confidentiality can be too severe to assume that employees learn and remember all that they need to know from this one session.

There are several ways that confidentiality can be breached. Leaving a message on a patient's answering machine may not seem to be breaching a confidentiality but it could have similar consequences to information overheard in an elevator. In addition to in-hospital breaches, employees should be educated in the danger of spreading patient information to friends and family outside of their work environment. In one literature source, a nursing aide assisted in the postoperative care of a fellow church member who has just had an abortion and then decided that it was her duty to confide in their minister.[2]

The following list of potential breaches was compiled from the initial survey as well as from input from the respondents and should be included in all training programs:

* Informal conversations between staff in public areas, including hallways, elevators, transport vans.

* Faxing to the wrong number

*Phone conversations in public areas that can be easily overheard

*Releasing patient information without permission

* Leaving messages on a patient's answering machine for anyone to hear

* Access to computer records

* Patient information left on copiers

* Unprotected patient charts left open in the public's view

* E-mail messages

2

Greve, P. (1990). Keep quiet or speak up? Issues in patient confidentiality. RN, 53 (12), 53.

* Talking about patients outside of the hospital

Obviously, there will always be confidentiality breaches that hospitals have no control over, no matter how much training they give employees. A disgruntled employee could take revenge through breaching patient records. Or, as one respondent pointed out, "faxing is our weakest point because you can't be accountable for who's on the other end."

However, if a hospital uses the proper medium to pass on the proper messages to all its employees, the chances of being caught with an uncomfortable situation is minimized. It's like crisis planning. It can help prevent the worst.

BIBLIOGRAPHY

1. Carman, D.M. (1996). Balancing patient confidentiality and release of information. IN Confidence, 4 (6), Retrieved October 1997 from the World Wide Web: http://www.ahima.org/publications/1a/nov.inconf.html

2. Carnall, D. (1995). Hospitals warn against stories between storeys. British Medical Journal, 311 (7004), 528.

3. Carpenter, J. (1997). Answers to confidentiality concerns. IN Confidence, 5 (5), Retrieved October 1997 from the World Wide Web: http://www.ahima.org/publications/1b/inconf.q-a.997.html

4. Coleman, M.T. (1995). Ensuring patient confidentiality. Journal of Family Practice, 40 (1), 18.

5. Corman, D., & Britten, N. (1995). Confidentiality of medical records: The patient's perspective. British Journal of General Practice, 45 (398), 485-88.

6. Cotton, P. (1986). Patient confidentiality: Peeking inside Pandora's box? Medical World News, 27 (19), 62-70.

7. Davis, A.J. (1981) Whom can you tell? American Journal of Nursing, 81, 2078.

8. Dennis, J.C. (1996). Are you at risk of breaching confidentiality? IN Confidence, 4 (2), 96, Retrieved October 1997 from the World Wide Web: http://www.ahima.org/publications/1a/jan-feb.inconf.html

9. Dodek, D. & Dodek, A. (1997). From Hippocrates to facsimile: Practicing patient confidentiality is more difficult and important than ever. Journal of the Canadian Medical Association, 156 (6), 847-852.

10. Dowd, S., & Dowd, L. (1996). Maintaining confidentiality: Health care's ongoing

dilemma. Health Care Supervisor, 15 (1), 24-31.

11. Fletcher, J.C., & Wertz, D. (1990). The price of silence. Hastings Center Report, 30 (3), 31-35.

12. Gostin, L. et al. (1997) "Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization," Retrieved October 1997 from the World Wide Web: http://www.epic.org/privacy/medical/cdc_survey.html

13. Grady, C., Jacob, J., et al. (1991). Confidentiality: A survey in a research hospital. Journal of Clinical Ethics, 2 (1), 25-30.

14. Greve, P. (1990). Keep quiet or speak up? Issues in patient confidentiality. RN, 53 (12), 53.

15. Hard, R. (1992). Keeping patient data secure within hospitals. Hospitals, 66 (20), 50.

16. Koska, M.T. (1992). Outcomes Research: Hospitals face confidentiality concerns. Hospitals, 66, 32-33.

17. Lawrence, L.M. (1994). Safeguarding the confidentiality of automated medical information. Joint Commission Journal on Quality Improvement, 20 (11), 639-646.

18. Lindenthal, J.J. & Thomas, C.S. (1982). Consumers, clinicians and confidentiality. Social Science & Medicine, 16, 333-35.

19. McKissock & Hoffman, PC. (1992). Laws and regulations affecting medical practice: A guide for Pennsylvania physicians, The PA Medical Society and the PA Medical Society Liability Insurance Co., June.

20. Milholland, D.K. (1994). Privacy and confidentiality of patient information. Journal of Nursing Administration 2, 19-24.

21. Morris, M.R. (1996). Patients' privacy on the line. American Journal of Nursing, 96 (10), 75.

22. Mortlock, T & Howell, M. (1994). Maintaining patient confidentiality in Admissions and Emergency. Nursing Times, 90 (34), 42-45.

23. Pelletier, M. (1995). Employee training: Keeping patient information confidential at a large hospital in a small town. IN Confidence, 3 (6), Retrieved October 1997 from the World Wide Web: http://www.ahima.org/publications/1a/nov-dec..inconf.html

24. Rhodes, H. (1996). Answers to confidentiality concerns. IN Confidence, 4 (3), Retrieved October 1997 from the World Wide Web: http://www.ahima.org/publications/1b/may-jun-q-a.html

25. Salladay, S.A. (1994). Patient confidentiality: On the spot. Nursing, 24 (8), 29-30.

26. Sharp, H. (1994). Letter to the editor. Journal of the American Medical Association, 271 (18), 1401-02.

27. Siegler, M. (1982). Confidentiality in medicine: A decrepit concept. New England Journal of Medicine, 307, 1518-21.

28. Simpson, R.L. (1994). Ensuring patient data, privacy, confidentiality and security. Nursing Management, 7, 18-20.

29. Smith, J. (1995). Confidentiality: Prying eyes. Nursing, 25 (9), 26.

30. Styffe, E. (1997). Privacy, confidentiality & security in clinical information systems. Nursing Administration Quarterly, 21 (3), 21.

31. Ubel, P., Zell, M., et al. (1995). Elevator talk: Observational study of inappropriate comments in public spaces. American Journal of Medicine, 99 (2), 190-94.

32. Weiss, B. (1982). Confidentiality expectations of patients, physicians and medical students. Journal of the American Medical Association, 247, 2695-97.

33. Woodward, B. (1995). The computer-based patient record and confidentiality. New England Journal of Medicine, 333 (21), 1419.

34. Office of Technology Assessment (1993). "The right to privacy in health care information," Retrieved October 1997 from the World Wide Web: http://www.eff.org/pub/privacy/medical/1993_ota_medical.privacy report.

35. News articles related to healthcare information security, Irongate, Inc. Retrieved October 1997 from the World Wide Web: http://www.irongateinc.com/html

APPENDIX

SURVEY QUESTIONS:

1. Does your hospital have a formal policy on patient confidentiality?

- ❑ Yes (Answer question 2)
- ❑ No (Skip to question 4)

2. If yes, how long has it been in place?

- ❑ Over 10 years
- ❑ 6-10 years
- ❑ 1-5 years
- ❑ Less than l year

3. How was the patient confidentiality policy developed?

- ❑ In house
- ❑ Consulting firm
- ❑ Other

_____

4. If you don't have a formal policy, are there patient confidentiality clauses within the general hospital policy?

- ❑ Yes
- ❑ No

5. How is the policy /clauses communicated to employees?
(please check all that are applicable)

- ❑ Through memos
- ❑ Through employee handbook
- ❑ Scheduled training programs
- ❑ Signs throughout hospital
- ❑ Confidentiality pledges requiring signature
- ❑ Other (please specify)

_____

MEMOS

6. If the policy is communicated through memos, do all employees (including physicians) receive these memos?

- ❑ Yes (Skip to question 6b)
- ❑ No (Skip to question 6a)

6a. If no, then who is excluded?

6b. If yes, must employees sign off that they have received and read the memo?

- ❑ Yes
- ❑ No

HANDBOOK

7. If the policy is communicated through a handbook, do all employees (including physicians) receive this handbook?

- ❑ Yes (Answer question 7a)
- ❑ No (Skip to question 7b)

7a. If yes, must employees sign indicating they have read the handbook?

- ❑ Yes (Skip to question 8)
- ❑ No (Answer question 7b)

7b. If no, who is excluded?

TRAINING PROGRAM

8. If you have a training program for patient confidentiality, how often does this training take place?

- ❑ Only when employee is hired
- ❑ Annually
- ❑ Both of the above (at start of employment and annually)
- ❑ Other

9. In the training program, what forms of communication are used to train employees? (please choose all that are applicable)

- ❑ Lecture
- ❑ Videos
- ❑ Role-playing
- ❑ Other _____

10. How long has this training program been in place?

- ❑ Less than a year
- ❑ 1-5 years
- ❑ 6-10 years
- ❑ Over 10 years

11. How was the training program developed?

- ❑ In house
- ❑ Consulting firm
- ❑ Other _____

12. Do all employees (including physicians) receive confidentiality training?

- ❑ Yes (Skip to question 13)
- ❑ No (Answer question 12a)

12a. If no, what level of employees are excluded?

13. Do all employees receive the same training?

- ❑ Yes (Skip to question 14)
- ❑ No (Answer question 13a)

13a. If no, please explain how training differs for the following types of employees:
a. Directly responsible for patient care (health care providers)

b. Indirectly responsible (ie, medical records, ward clerks)

c. No direct patient care (ie, maintenance)

POTENTIAL BREACHES

14. Either through an employee handbook, a memo or training program, does your hospital address how confidentiality could be breached through: (please check all that are applicable)

- ❑ Informal in-hospital conversations that can be overheard
- ❑ Phone conversations that can be overheard
- ❑ Leaving sensitive information on message machines in a patient's home
- ❑ Faxing (ie, wrong number, sending sensitive information)
- ❑ Releasing patient information to family and/or friends
- ❑ Patient charts (left out in the open, unprotected)
- ❑ Use of copier machine
- ❑ Computerized records
- ❑ Other areas _____

15. Do you discuss with employees what is an authorized release of patient information to legal recipients, ie, other hospitals and care providers, insurers, in response to subpoenae?

- ❑ Yes
- ❑ No

16. Is there a written plan in place to deal with suspected breaches of confidentiality?

- ❑ Yes
- ❑ No

16a. If yes, is this plan communicated to employees?

- ❑ Yes
- ❑ No

17. Is there any information not covered in this survey that you would like to add about

patient confidentiality and employees?

Demographics

Number of employees: _____

Number of beds: _____

Does hospital have an academic affiliation? ❑ Yes ❑ No

Would you like a copy of the:
Survey results ❑ Yes ❑ No
Thesis ❑ Yes ❑ No

Thank you.